# Department of Homeland Security
# Information Analysis and Infrastructure Protection
# Daily Open Source Infrastructure Report for 11 July 2003

Current Nationwide Threat Level is


For info click here
www.whitehouse.gov/homeland

## Daily Overview

- IDG News Service reports that in a rising trend of "brand spoofing" scams, a new Web site spoofs the PayPal Inc. online payment site and attempts to trick PayPal customers into divulging sensitive account and billing information. (See item 6)
- The Trucker reports the National Tank Truck Carriers Association has issued a warning about an individual with a forged Florida Commercial Driver's License. (See item 9)
- Microsoft has released "Security Bulletin MS03−023: Buffer Overrun In HTML Converter Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item 20)
- Microsoft has released "Security Bulletin MS03−024: Buffer Overrun in Windows Could Lead to Data (Important)," and a patch is available on the Microsoft Website. (See item 21)
- Microsoft has released "Security Bulletin MS03−025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation (Critical)," and a patch is available on the Microsoft Website. (See item 22)

**DHS/IAIP Update *Fast Jump***

**Production Industries:** Energy; Chemical; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information and Telecommunications; Internet Alert Dashboard
**Other:** General; DHS/IAIP Web Information

# Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 09, The San Diego Union−Tribune* — **San Diego judge approves shipments of Mexican electricity to United States. A San Diego federal judge refused yesterday to halt shipments**

**of electricity to the United States from two new power plants in Mexico, striking a blow to an environmental group that sought to shut off the cross−border power flow.** Judge Irma E. Gonzalez said the plants near Mexicali can continue to pump power across the border while the U.S. Department of Energy works to come into compliance with the National Environmental Protection Act. The Border Power Plant Working Group went to court seeking to stop electricity from flowing over power lines connecting the Mexicali plants to the Southern California power grid, among other measures. **Gonzalez found that the group failed to prove that shipping power over the lines would do substantial environmental harm during the year she gave the Energy Department to comply with the federal law.** Gonzalez's ruling is the latest salvo in a complex battle over power plants in Mexico that supply electricity to the Southwest. Critics contend energy companies are building power plants just across the border to avoid tough U.S. environmental laws. **These two plants, built by San Diego's Sempra Energy Resources and Burlington, Mass.−based InterGen, can deliver about 1,600 megawatts of electricity to U.S. consumers or enough to power about a million households.**
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3977579

2. *July 09, San Jose Mercury News* — **Oil fire at California power plant threatens nearby wildlife refuge. At least a million gallons of residual oil inside an abandoned fuel tank at Duke Energy's Moss Landing power plant caught fire Tuesday, blanketing central coast skies with acrid black as fire crews battled the blaze precariously close to a national wildlife sanctuary. A "shelter in place" advisory for residents to stay indoors continued into the night, hours after the fire was reported at 4:12 p.m. at the property on Highway 1 in Monterey County.** The region's largest power plant is across the coastal highway from the Moss Landing Harbor and just south of the Elkhorn Slough National Estuarine Research Reserve. No injuries were reported and no evacuations were ordered in the early evening. The fire also did not affect the power plant's operation. **It was not known how the fire ignited in the 150−foot−wide, 40−foot−tall tank. In the 1990s, the plant converted to natural gas, leaving the oil storage tanks unused.** As black smoke and flames spewed from the tank, researchers at neighboring Elkhorn Slough −− where great blue herons, great egrets and double−crested cormorants are nesting −− could only hold their breath and hope for the best. It is also not known what effect the smoke has had on area residents.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3977599

3. *July 09, Business Wire* — **West Virginia Governor dedicates largest wind farm in the East.** West Virginia Governor Bob Wise today joined FPL Energy, Exelon Corporation and about 150 guests in Tucker County to dedicate the largest wind farm east of the Mississippi River along the windy ridge of Backbone Mountain north of Thomas, WV. Governor Wise was joined by FPL Energy's Senior Vice President of Development Michael O'Sullivan, Exelon Generation Vice President of Government Affairs Jan Freeman, and more than 150 local and regional guests to celebrate the largest wind farm in the Eastern United States and the organizations that helped bring the facility to West Virginia. **The Mountaineer Wind Energy Center is capable of generating enough electricity to power 22,000 homes. Construction of the 44 wind turbines at the wind farm, each about 228 feet tall to the center of the blade hub, began in the summer of 2002 and was completed in December.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=comtex_2003_07_09_bw_0000−0815−fl−fpl−energy &SMContentSet=0

4. *July 09, Associated Press* — **Energy Dept. halts nuclear shipments plan. A plan to ship nuclear waste from Nevada to New Mexico through Southern California was canceled Wednesday because of opposition from state officials, the Department of Energy (DOE) said.** It marked the first time shipment plans have been halted because of a state's resistance, DOE spokesman Joe Davis said. There were no immediate plans to reschedule the truck shipments of medium−level waste on the circuitous 300−mile route through California. **The DOE decision came after the Western Governors' Association notified the agency that California did not concur on the route. The agency's protocol is to get a state's agreement before shipping, Davis said.** "This is not a delay," he said. "We're canceling the shipments until the Western Governors' Association and the state of California and state of Nevada can engage together and propose a meaningful compromise." **The primary objection was the roundabout route, from Nevada through California and Arizona to a disposal facility in New Mexico. Part of the trip was along state Highway 127, a former wagon road that authorities said was not designed for heavy trucks, is poorly maintained in places and is popular with tourists heading to Death Valley.**
   Source: http://www.washingtonpost.com/wp−dyn/articles/A34922−2003Jul 9.html

5. *July 08, The Philadelphia Inquirer* — **Pennsylvania nuclear power plant to use wastewater from coal mines.** Coal mines dump millions of gallons of unwanted wastewater into rivers every day. A nuclear plant needs millions of water a day for its cooling process. While the two have tried to work things out before, the deal always fell through. Not this time. **By the end of this month, the Limerick nuclear power plant will reduce its take from Point Pleasant on the Delaware River, turning instead to wastewater from a coal mine in Schuylkill County. "It's a very novel and innovative concept," Cathleen Meyers, Delaware River Basin commissioner, said before voting to approve a four−to−five−month trial run of the plan last month.** The basin commission unanimously approved the trial after a hearing in Trenton. To address concerns about possible water contamination from the coal mine and soil erosion, commissioners approved additional water testing and said they could halt the trial run if any problems ensued. Overall, state, nuclear and environmental groups seemed pleased with the Limerick plan.
   Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3977514

[Return to top]

## Chemical Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

Nothing to report.
[Return to top]

## Banking and Finance Sector

6. *July 10, IDG News Service* — **New site spoofs PayPal to get billing information.** A new Web site spoofs the PayPal Inc. online payment site and attempts to trick PayPal customers into divulging sensitive account and billing information. The fake Web site is the latest example in what security experts say is a rising trend of "brand spoofing" scams. **PayPal customers are directed to the site, www.paypal−billingnetwork.net, by an e−mail message that appears to come from the Mountain View, California, company. The message claims that due to a "recent system flush," the customer's billing and personal information is "temporaly unavailable" (sic). Customers need to verify their identity by visiting the site or risk having their account canceled, according to the message, which is signed by "Jhon Krepp" from the "PayPal Billing Department."** The actual site is almost identical to PayPal's real site, with the same graphics, layout and wording. In fact, many of the links on the site point back to the actual PayPal Web site. PayPal could not be reached for comment about the scam site.
   Source: http://maccentral.macworld.com/news/2003/07/09/paypal/

7. *July 10, New York Times* — **Serial brides charged in New York 'green card' scam. Six women who were paid $1,000 a pop to marry 43 immigrants and help them get "green cards" have been charged with lying to obtain marriage licenses, officials said on Wednesday.** "They are nothing more than career brides," said Victor Robles, the city clerk tasked with issuing and tracking marriage licenses who uncovered the scam about two years ago. The so−called green card is actually a coveted resident alien identification card that allows immigrants to live and work in the United States and eventually to apply for U.S. citizenship. Marriage to a U.S. citizen is one of the easiest ways for a foreigner to obtain a "green card." **Robles said he began investigating the case when he heard that a woman was claiming to have been married six times. He discovered there was no system to see if someone had obtained more than one marriage license in a single year. Robles changed the system so that he could search 10 years of city records and found that the six women had applied for a total of 43 marriage licenses.** The husbands came from countries including Pakistan, Ecuador, the Dominican Republic, Peru, Trinidad, St. Lucia, India, Nigeria and other parts of Africa.
   Source: http://www.nytimes.com/reuters/news/news−crime−brides.html

8. *July 09, Associated Press* — **Feds: SSA vulnerable to identity theft. Congressional investigators working undercover obtained Social Security numbers for nonexistent newborns and used the Social Security numbers of dead people to obtain drivers licenses, exposing weaknesses at the Social Security Administration that could be exploited by identity thieves.** The thieves use a person's personal information, such as a Social Security number or credit card number, to establish a false name or citizenship, purchase goods or fraudulently apply for credit. Investigators from the General Accounting Office, Congress' investigative arm, used counterfeit documents to build fake identities that included Social Security numbers. **In the undercover investigations, fake birth certificates and baptismal certificates were used to obtain Social Security numbers for infants.** Social Security policies do not require that the agency's workers verify documents used to prove the identity of children younger than one year old. False documents also got past employees at driver's license facilities. **A Social Security Administration program designed to verify the numbers for state driver's license facilities failed to alert the employees that the numbers came from**

**deceased individuals.**
Source: http://www.washingtonpost.com/ac2/wp−dyn/nation/latestap?sta rt=80&per=20

[Return to top]

## Transportation Sector

9. *July 10, The Trucker* — **Truckers asked to watch for driver with fake Commercial Driver's License. The National Tank Truck Carriers Association (NTTC) issued a warning June 30 about a forged Commercial Driver's License (CDL).** A member company of NTTC, located in the southeastern United States, reported that an individual applied for employment using a forged Florida CDL. **The applicant presented the CDL, number B300−061−81−343−0, using the name Bilal Ahmed Bhutta. The person applied for employment as a driver. A Social Security Card was also presented with the notation "Valid for work only with INS authorization."** The applicant inquired as to the type of products hauled by the carrier. Anyone encountering an individual using this identification is asked to take no direct action, but to contact the local FBI Joint Terrorism Task Force office or other appropriate authorities.
Source: http://www.thetrucker.com/stories/07_03/0709_fake.html

10. *July 10, New York Times* — **New Jersey's new driver's license is delayed. In April, New Jersey Gov. James E. McGreevey announced that state motor vehicle offices would start issuing new plastic driver's licenses in late July, to replace the current paper licenses that are among the easiest in the nation to counterfeit. But today, officials said that the state's six million drivers would have to wait at least until the end of September.** Diane Legreide, chief administrator of the State Motor Vehicle Commission, attributed the delay to security concerns, untrained workers and unfinished network wiring at motor vehicle offices. The McGreevey administration has embarked on a restructuring of the agency, which it has faulted for poor customer service and the troubled start of the emissions−testing system in 1999. **Ms. Legreide said an investigation discovered inaccuracies in almost 1.1 million licenses. For instance, many Social Security numbers in the agency's database do not match the Social Security database.** The new licenses will have a number of security features, including a magnetic strip and holograms.
Source: http://www.nytimes.com/2003/07/10/nyregion/10LICE.htm

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

11. *July 10, United Press International* — **USDA urged to employ mad cow rapid test. Although the U.S. Department of Agriculture (USDA) maintains American cattle are free of mad cow disease, critics say there is no way to know for certain until the agency implements**

**rapid tests.** The critics, including a former rancher and a former USDA veterinarian, said the tests, which yield results in a matter of hours, would enable the agency to screen millions of animals. **So far, the USDA has been reluctant to use the rapid test, claiming its current method, which can take eight days to produce results, is adequate to conduct the sufficient levels of surveillance.** Last year, the USDA screened 20,000 cattle out of the more than 30 million slaughtered. **Critics charge the USDA's system, because it tests so few animals, makes it unlikely mad cow would ever be detected. The USDA defends its use of the slow test, calling it the "gold standard" and the most accurate. "We can use the best test out there and still do a high level of surveillance in the U.S.," said USDA spokesman Ed Curlett, noting the agency's current level of testing is sufficient to detect mad cow disease even if it was occurring in only one cow per million.**
Source: http://www.upi.com/view.cfm?StoryID=20030708−044102−7940r

12. *July 10, Evening Standard* — **Chicken shortage as flu hits flocks. The price of chicken has doubled at some wholesale butchers after bird flu wiped out poultry flocks in Europe. Wholesalers are reporting chicken prices at a 30−year peak as demand outstrips supply.** The flu spread through flocks in Holland and Belgium, home to some of the biggest poultry producers in the world. They supply the UK with 150,000 tons of meat a year. In the past three months, the wholesale−cost of chicken has soared after the industry turned to UK producers to fill the shortfall. Steve Crosby, who owns SC on Charterhouse Street, one of the City's leading butchers, said: "We sell five−kilogram bags of chicken and three months ago they were going for about £12.50. Now they are selling for £25. "It is dearer than I have ever seen it." **There are fears that the rise may be passed on to supermarkets and restaurants." If the rise spreads, it raises the prospect of a kilo of free−range chicken increasing from around £4.95 to almost £10.**
Source: http://www.thisislondon.co.uk/news/articles/5683820?source=E vening%20Standard

13. *July 10, Canadian Press* — **Cattle surplus may force producers to kill cows. Faced with a growing cattle surplus, producers may have to start killing their cows if borders with Canada's key trading partners don't open soon, say industry experts.** The only other alternative is to more than double Canadian beef consumption to about 35 kilograms per person each year and increase the slaughter of cattle by Canadian packing plants. **Cor Van Raay of Picture Butte, Canada's largest cattle feeder, said Canadian packers won't be able to slaughter all the animals, especially when surplus stocks peak at the end of July or early August. "Price or no price, I do not know where these cattle can go," said Mr. Van Raay. "There will be too many cattle to physically kill in Canada.** Some time down the road, we will have to get rid of some cattle and I suggest depopulation of cattle." Anne Dunford, a market analyst with Canfax, said Canadian packers were killing about 70,000 beef animals every week before the discovery. In the five weeks after May 20, national slaughter dropped to a range of 28,000 to 39,000 a week. "I hope they will be closer to 50,000 a week that is needed to satisfy the middle−carcass demanded by Canadian consumers," said Ms. Dunford. **But that won't cut into the burgeoning cattle surplus, she warned. That would take a slaughter of 80,000 a week and would take months.**
Source: http://www.globeandmail.com/servlet/story/RTGAM.20030710.wco ww0710/BNStory/National/

[Return to top]

## Food Sector

**14.** *July 10, New York Times* — **Meat inspections declining.** Federal border inspections of imported meat and poultry are declining as Congress is calling for increased surveillance to prevent bioterrorism and improve the safety of meat consumed in the nation. **The U.S. Department of Agriculture (USDA) began a new inspection system last fall and reduced the percentage of meat crossing the border that is inspected to six percent from 17 percent, department records show. "Yes, the amount of meat inspected is less, but the meat we inspect is inspected more thoroughly," said Karen Stuck, administrative assistant for international affairs at the food safety inspection service at the department.** The reduction in border inspections is included in a report on the effect of trade rules on national food safety requirements to be released on Thursday by Public Citizen, a consumer group. Mary Bottari, author of the report, said it was unclear how the USDA could justify sampling far less meat when the amount of meat imported into the United States had increased to 4 billion pounds in 2002 from 2.5 billion pounds in 1997. **With less meat inspected, the amount of meat rejected has dropped to 712,744 pounds from 2.1 million pounds, according to the agriculture agency's last two quarterly reports.**
Source: http://www.nytimes.com/2003/07/10/national/10MEAT.html

[Return to top]

## Water Sector

**15.** *July 10, Water Tech Online* — **Nitrate−removal water study to focus on NYC supply. Commissioner Christopher O. Ward of the New York City Department of Environmental Protection (DEP), announced that the DEP will participate in a demonstration study to determine the feasibility of constructing a full−scale facility for the biological treatment of high ammonia waste streams.** Known as the SHARON Process, it is a biological treatment technique to handle high ammonia waste streams, developed in the Netherlands. It works by altering the normal microbiology to produce nitrogen gas from nitrite rather than nitrate. This process reduces the hydraulic retention time required as well as chemical and energy costs over that needed by conventional processes. "We are hopeful that innovative processes, such as the SHARON Process, will help the DEP avoid the high costs usually associated with nitrogen removal," said Ward. Alfonso Lopez, Deputy Commissioner of DEP's Bureau of Wastewater Treatment said, **"If the demonstration project proves to be successful, the DEP will implement the facility as part of its treatment technology, the first of its kind in the United States."**
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=41593

**16.** *July 09, Associated Press* — **New device could help track underground water flows.** That torpedo−like device hanging a hundred feet or so below the belly of a low−flying helicopter is a new technology that scientists hope will aid in the tracking of underground water flows. From Tuesday through the weekend, crews involved in joint project of the federal Mine Safety and Health Administration and the National Technology Transfer Center at Wheeling Jesuit University will be testing the device over 13 coal waste impoundments in seven southern West

Virginia counties. **The sensor uses electromagnetic waves, much like radio waves, to track the flow of water underground. When the electromagnetic waves emitted by the device hit something conductive, such as underground water, they are reflected back and mapped by the computer.** Although the device is designed to track underground flows as deep as 300 feet below the surface, in practice it has only tracked flows about 150 feet down. **The device has already helped find the source of contamination to Clear Lake, CA, the largest natural lake in that state. Investigators could not locate the source of pollution to the lake, which was separated from an old mercury mine of the 1880s by a dam made of refuse from the old mine.**
Source: http://www.zwire.com/site/news.cfm?BRD=1078&dept_id=151021&newsid=9497349&PAG=461&rfi=9

[Return to top]

## Public Health Sector

17. *July 10, Associated Press* — **Researchers find test for bioweapons. Sensors that light up within seconds after coming into contact with a dangerous virus or bacteria may allow emergency workers in the field to quickly detect any weapons of bioterrorism, researchers say. In a study, Massachusetts Institute of Technology (MIT) researchers say they have engineered cells that are able to sense and identify bioweapons spread through the mails, air, or water.** The system uses mouse B lymphocytes that have been engineered to contain a jellyfish gene for a luminescent protein and altered to carry antibodies that respond to specific diseases. When antibodies on the sensor cells detect a pathogen, such as anthrax, they trigger a burst of calcium within the B cells. Within seconds, the calcium activates the bioluminescent protein and causes the whole cell to glow. This is a signal that the specimen has a dangerous germ. **The system would not require advanced training to operate, in contrast to current lab techniques that are performed by highly trained scientists or technicians. Todd H. Rider, an MIT researcher, said the system, developed with funding from the Defense Advanced Research Projects Agency, has been tested successfully against all of the known pathogens that can be used for bioweapons, including anthrax, smallpox, plague, tularemia, and encephalitis.**
Source: http://www.sunherald.com/mld/sunherald/news/breaking_news/62 74103.htm

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

18. *July 10, Government Computer News* — **FEMA helps suburban emergency center open for business.** Through a donation of 15 desktop PCs and software from the Homeland Security Department, Laurel, MD, government officials today are launching a new Emergency

Operations Center to become a regional coordination hub for four counties surrounding Washington. **Maryanne Anthony, Laurel's director of IT and community services, said the center is the first of its kind in the nation with regional capabilities. She said it will let the neighboring counties communicate with the federal government and some large corporations through a secure network using the Disaster Management Interoperability Services software.** DHS modified the application from the Marine Corps.' Consequence Management Interoperability Services Suite. DMIS also is used on the Disasterhelp.gov site, which is a part of the Disaster Management e−government project that Homeland Security is managing. **The software provides users with a real−time continuous log of activity during the emergency. Officials can pull up detailed maps and overlay them with specific landmarks, waterways or buildings. Anthony said the software also can show evacuation routes and shelters, and can outline the affected area.**
Source: http://www.gcn.com/vol1_no1/homeland−security/22713−1.html

19. *July 09, Baltimoree Sun* — **Terror drill to test area response. Health officials are planning an extensive bioterrorism drill in the Baltimore, MD area that will send volunteers, wearing makeup and acting as though they have been infected with smallpox or other diseases, to area hospitals. The exercise will test the communications systems that link more than a dozen area hospitals to city, county, and state emergency officials.** Organizers wouldn't reveal when the practice will start, noting that they want to maintain some element of surprise. But they said the drill will occur soon and that the public should be aware so that people won't panic and get hurt. The volunteers, who will pretend to have symptoms of diseases, will wear shirts proclaiming "this is only an exercise" so that doctors won't be tricked into abandoning patients with real health emergencies to attend to actors, officials said yesterday. **The doctors will have to figure out which disease or diseases the actors have, based on their descriptions of their symptoms and their makeup.** Donald Keldsen, director of the Maryland Emergency Management Agency, said one aim of the exercise is to help train state, city, and county officials to communicate with each other during a crisis. The practice will involve 200 volunteers from Civic Works, a nonprofit organization, and 15 area hospitals.
Source: http://www.sunspot.net/news/custom/attack/bal−md.bioterror09jul09,0,7258763.story?coll=bal−local−headlines

[Return to top]

## Information and Telecommunications Sector

20. *July 09, Microsoft* — **Microsoft Security Bulletin MS03−023: Buffer Overrun In HTML Converter Could Allow Code Execution.** There is a flaw in the way the HTML converter for Microsoft Windows handles a conversion request during a cut−and−paste operation which results in a vulnerability. **A specially crafted request to the HTML converter could cause the converter to fail in such a way that it could execute code**. **An attacker could craft a specially formed Web page or HTML e−mail that would cause the HTML converter to run arbitrary code on a user's system**. If Internet Explorer Enhanced Security Configuration has been disabled, the protections put in place that prevent this vulnerability from being automatically exploited would be removed. **Exploiting the vulnerability would allow the attacker only the same privileges as the user. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch**

**immediately.**
**Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−023.asp**

21. *July 09, Microsoft* — **Microsoft Security Bulletin MS03−024: Buffer Overrun in Windows Could Lead to Data Corruption.** When a client system sends an Server Message Block (SMB) packet to the server system, it includes specific parameters that provide the server with a set of "instructions." The server is not properly validating the buffer length established by the packet. If the client specifies a buffer length that is less than what is needed, it can cause the buffer to be overrun. **By sending a specially crafted SMB packet request, an attacker could cause a buffer overrun to occur. If exploited, this could lead to data corruption, system failure, or it could allow an attacker to run the code of their choice**. An attacker would need a valid user account and would need to be authenticated by the server to exploit this flaw. By default, it is not possible to exploit this flaw anonymously. The attacker would have to be authenticated by the server prior to attempting to send a SMB packet to it. **Blocking port 139/445 at the firewall will prevent the possibility of an attack from the Internet. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators consider installing the patch**.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−024.asp

22. *July 09, Microsoft* — **Microsoft Security Bulletin MS03−025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation.** Microsoft Windows messages provide a way for interactive processes to react to user events and communicate with other interactive processes. **A flaw in the way that the Microsoft Accessibility Utility Manager handles Windows messages results in a vulnerability** because the control that provides the list of accessibility options to the user does not properly validate Windows messages sent to it. It's possible for one process in the interactive desktop to use a specific Windows message to cause the Utility Manager process to execute a callback function at the address of its choice. **Because the Utility Manager process runs at higher privileges than the first process, this would provide the first process with a way of exercising those higher privileges**. By default, the Utility Manager contains controls that run in the interactive desktop with Local System privileges. **An attacker who had the ability to log on to a system interactively could run a program that could send a Windows message upon the Utility Manager process, causing it to take any action the attacker specified**. This would give the attacker complete control over the system. **Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.**
**Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−025.asp**

## Internet Alert Dashboard

**Current Alert Levels**

| | |
|---|---|
|  AlertCon: 1 out of 4 https://gtoc.iss.net |  Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/ |

**Current Virus and Port Attacks**

| | |
|---|---|
| **Virus:** | #1 Virus in the United States: **JS_NIMBDA.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 137 (netbios−ns), 80 (www), 445 (microsoft−ds), 1434 (ms−sql−m), 113 (ident), 139 (netbios−ssn), 4662 (eDonkey2000), 0 (−−−), 2397 (ncl), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

# General Sector

**23.** *July 10, Washington Post* — **Corporate security funding up slightly.** Corporate spending on security measures has increased only slightly in the wake of the September 11, 2001, terrorist attacks, according to a new study released on Wednesday by an organization representing company security managers. **The nationwide survey of more than 330 security officials at large corporations, funded by ASIS International, found just a four percent median increase in spending for corporate security since the attacks on the World Trade Center and the Pentagon. The median represents the point at which half those surveyed spent more than four percent on security, and half less.** The study broadly assessed spending on security measures, looking at physical protection of employees and facilities, computer security, and financial risk management. Thomas E. Cavanagh, author of the report and a security specialist at the Conference Board, the business research group that conducted the survey, cited the nation's economic downturn as a primary reason security spending has not been higher. **For the past four years, workplace violence was considered the No. 1 security threat among Fortune 1000 companies, according to a survey by security consulting firm Pinkerton. Terrorism ranked fourth in the 2003 survey.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A35362−2003Jul 9.html

**24.** *July 10, Reuters* — **Chicago man arrested as alleged Iraqi agent.** A 60−year−old writer and publisher was arrested at his Chicago area home on Wednesday and charged with providing information to Saddam Hussein's intelligence agency about the deposed Iraqi leader's foes. **Khaled Abdel−Latif Dumeisi, who has a Jordanian passport but has lived in the United States for about 10 years, was described in an affidavit as an ``unregistered agent'' for the former Iraqi government who reported on Iraqi exile leaders and gave press identification cards to Iraqi intelligence agents.** In one alleged case, Dumeisi was trained by the Mukhabbarat, the Iraqi intelligence agency, to use a pen with a hidden camera and microphone

to secretly record an interview with an unnamed member of the Iraqi opposition. ``We're not saying he's the greatest spy that ever lived," said Patrick Fitzgerald, the U.S. attorney for the Northern District of Illinois. ``But I'm also telling you we can't have people going around the country gathering information ... and giving it to the Iraqi intelligence service."
Source: http://www.nytimes.com/reuters/news/news−iraq−usa−agent.html

25. *July 10, Reuters* — **Bomb blast kills security officer in Moscow center.** A Russian security officer was killed on Thursday trying to defuse a bomb planted at a central Moscow restaurant by a suspected woman Chechen separatist. **Moscow has been on terror alert since Saturday when two women, said to be Chechens, blew themselves up at an open−air rock festival, killing 14 people and themselves. The latest blast −− on Moscow's main shopping street −− fueled fears that conflict between Russian forces and Chechen rebels was once again spilling onto the streets of the capital despite a new Kremlin peace plan.** The woman brought the bomb in a bag to the Imbir restaurant on Tverskaya Street late on Wednesday and threatened to blow up the place after she was barred from entering. She then dumped the bag on the pavement and was detained as she fled, a police spokeswoman told Reuters. She said security officers failed to dispose of the device by remote control and it detonated while a security officer −− who helped disarm one bomb at Saturday's rock festival −− was trying to defuse it by hand just outside the restaurant.
Source: http://www.nytimes.com/reuters/news/news−russia−blast.html

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

**DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129 |
| Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information. |

## Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

## DHS/IAIP Disclaimer